

In re Application of WILLMAN
Serial No. 09/915,628

REMARKS

The Final Office action has been carefully considered. Claims 1-77 were rejected under 35 U.S.C. § 112, second paragraph, for being indefinite for failing to point out and distinctly claim the subject matter which the applicant regards as the invention. Claims 1-5, 7-34, and 36-77 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Magee et al., U.S. Patent No. 5,729,710 (hereinafter "Magee") in view of Williams U.S. Patent No. 6,304,973 (hereinafter "Williams"). Claims 6 and 35 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Magee in view of Williams, and in further view of Gulsen U.S. Patent No. 5,727,211 (hereinafter "Gulsen"). Entry of the response and reconsideration of the claims under the provisions of 37 C.F.R. 1.116 is earnestly solicited.

By previous amendment, the Abstract and claims 70 and 74-75 were amended. By the present amendment, claims 1, 32, 65, and 76 have been amended and claims 31, 69 and 77 have been canceled. Applicant submits that the claims 1-77 as initially presented were in acceptable form. Independent claims 1 and 32 and dependent claims 65 and 76 have been amended to more particularly point out and distinctly claim the invention. Applicant further submits that the claims as filed were patentable over the prior art of record, and that the amendments herein are for purposes of clarifying the claims and/or for expediting allowance of the claims, and not for reasons related to patentability. Applicant respectfully traverses the Examiner's arguments in the Final Office action dated June 27, 2005. Reconsideration is respectfully requested.

Turning to the 35 U.S.C. § 112 rejections, the Office action has rejected independent claim 32 for antecedent basis issues, independent claims 1, 32, and 64 and

In re Application of WILLMAN
Serial No. 09/915,628

dependent claim 76 for indefiniteness, as well as dependent claims 31, 69, and 77 for limiting the method claims to computer readable medium claims. Applicant has amended claims 1, 32, 64, and 76, canceled claims 31, 69, and 77, and respectfully traverses these rejections.

Turning to the 35 U.S.C. § 103(a) rejections, one or more aspects (hereinafter “aspects”) of the subject matter disclosed and/or claimed by applicant relate to providing memory security (sometimes referred to as “curtained memory”) and overcomes other memory-related problems by restricting existing code, such as drivers, without changing that code and without changing existing microprocessors. In aspects, this may be accomplished by enabling processes to have multiple memory maps, with any given thread (unit of execution) of a process being associated with one of the maps at any given time. This may provide memory isolation without requiring a process switch. In addition to providing isolation among the various divisions of code (e.g., procedures or drivers) executed by threads within the same process, which eliminates some memory access bugs, multiple maps for a single process may be used to provide curtained memory. To this end, memory isolation may be combined with controlled, closed memory map switching by trusted code to selectively limit the memory addresses that the threads of a process can access. For example, the threads of the process may ordinarily run at one privilege level, while map switching is only allowed at a higher privilege level. Since threads run through code, the map may be changed on entering or leaving certain verified and trusted code, thus controlling what memory addresses a thread can access based on what code is being executed at a given time. In this manner, only a small amount of trusted code decides what

In re Application of WILLMAN
Serial No. 09/915,628

virtual memory a given thread can access and when, thus providing curtailed memory without changing the microprocessor design.

Aspects of the subject matter disclosed and/or claimed by applicant may be implemented with any microprocessor that has protection and a protection-context-change mechanism. For example, in an x86 processor, the protection mechanism may comprise a call gate, with map switching not allowed except at a ring 0 privilege level. To change a map for a given code module, which operates at a ring 1 or higher privilege level, a hardware call gate switches to ring 0, where it executes code that switches the map such as to access protected memory, and then calls a predefined service entry point (e.g., a system API) on behalf of the code module. On return from the called service, the privilege level is restored to ring 1 and the code module is returned to a different map (e.g., different access) on exit. Note that the process (threads) request allocation of memory as before, but trusted code (e.g., as part of the operating system) is in control of which map (e.g., Map0 or Map1 in a two-map process) each thread receives. To provide a truly-safe protection mechanism, certain data structures also may need to be protected, (e.g., the tables that determine the virtual-to-physical memory address mapping need to be protected from write access by untrusted processes), otherwise an untrusted process could simply change the table data (e.g., the mappings therein) to access otherwise protected memory.

Note that the above description is for informational and example purposes only, and should not be used to interpret the claims, which are discussed below.

In contrast, Williams does not deal with changing a privilege level to a level that allows a memory map change responsive to a request via a process thread associated with a first memory map, performing the map change to associate a second memory map with the

In re Application of WILLMAN
Serial No. 09/915,628

process thread wherein the second memory map provides different memory access with respect to the first memory map, and restoring the privilege level to a level that does not allow a map change. Rather, Williams is directed towards solving an entirely different problem, essentially:

To overcome the limitations of the conventional security mechanisms. It is a further object of the invention to provide a secure network in which the security mechanisms are at layer 3 of protocol hierarchy. It is another object of the invention to provide a centralized administration of a layer 3 secure network that may be distributed over the Internet. It is another object of the invention to provide a security device that prevents unauthorized third parties from gaining access to a host. It is another object of the invention to provide a multi-level secure network having a security device coupled between each host and the network medium. Williams, col. 4, lines 26 – 35.

In other words, Williams describes a hardware network having two major components: a Network Security Center (NSC) and security network interface cards or devices. The network allows trusted users to access outside information, including the Internet, while stopping outside attackers at their point of entry. Williams, Abstract and col. 4, line 26 – col. 5, line 13. Williams further describes, “(t)he security device is a separate hardware board having a separate CPU, memory, network interface and bus architecture from the application processes on the host. A dual-ported RAM architecture guarantees that no malicious host process can tamper with the internal configuration of the security device. All network accesses must go through a security device, which implement security mechanisms for each and every access attempt. The security devices cannot be bypassed since there is no other path to or from the network.” Williams, col. 5, lines 33 – 42.

Moreover, Williams discloses, “(t)he network extends the mediation and cryptographic protection offered by a firewall (with its mediation and its cryptographic

In re Application of WILLMAN
Serial No. 09/915,628

protection) to the network interface of each individual host computer.” Williams, col. 5, lines 43 – 46. To that end, Williams discloses, “(t)he network provides hardware based mediation (MAC and DAC) at each host, and provides cryptographic protection (secrecy, integrity) on all host-to-host associations.” Williams does not disclose, suggest, or remotely hint at responding to a request via a process thread associated with a first memory map to change a privilege level to a level that allows a memory map change as claimed by applicant. Nor does Williams disclose, suggest, or remotely hint at performing the memory map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread, and restoring the privilege level to a level that does not allow a map change also as claimed by applicant. In other words, providing the mediation and cryptographic protection offered by a firewall to the network interface of each individual host computer is far different than performing a map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread and restoring the privilege level to a level that does not allow a map change.

Furthermore, Magee does not cure the deficiencies of Williams. In any possibly permissible combination with Williams, Magee and Williams do not disclose or suggest: receiving a request via a process thread having a first memory map associated therewith; changing a privilege level to a level that allows a map change; performing the map change to associate a second memory map with the process thread, the second memory map providing different memory access with respect to the first memory map; and restoring the privilege level to a level that does not allow a map change. Thus, in any permissible combination, the cited references still fail to disclose or suggest applicant’s invention.

In re Application of WILLMAN
Serial No. 09/915,628

By law, in order to establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In addition, "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Further, if prior art, in any material respect teaches away from the claimed invention, the art cannot be used to support an obviousness rejection. *In re Geisler*, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed Cir. 1997).

Turning to the rejection of independent claim 1 of the present invention, claim 1 generally recites receiving a request via a process thread having a first memory map associated therewith, changing a privilege level to a level that allows a map change, performing the map change to associate a second memory map providing different memory access with respect to the first memory map with the process thread, and restoring the privilege level to a level that does not allow a map change.

The Office action cites Magee (col. 18, lines 28-44) to allege that Magee discloses "receiving a request via a process thread having a first memory map associated therewith" Office action, pg. 4, sec. 5. The Office action further cites Magee (col. 15, lines 10-34, col. 18, lines 43-44, col. 9, lines 40-56, col. 33, lines 53-61) to allege that Magee discloses "various privilege levels with maps." Office action, pg. 4, sec. 5. The Office action concedes that "Magee fails to explicitly teach changing maps, performing the map change to associate a second memory map with the process thread, the second memory providing different memory access with respect to the first memory map; and restoring the privilege level to a level that does not allow a map change." Office action, pg. 4, sec. 5. Again, Applicant submits that Williams, in any permissible combination with Magee, does not cure

In re Application of WILLMAN
Serial No. 09/915,628

these significant deficiencies. The Office action cites Williams (col. 26, lines 18-26) to allege that Williams "teaches mapping and switching back and forth between separate trusted and non-trusted systems (col. 26, lines 18-26)." Office action, pg. 4, sec. 5. The cited text of Williams reads, "(t)he second host 88 has a security device 18 that permits the host 88 to operate either on the second VPN 82 or on an untrusted line 84. This ability to switch between a trusted network 82 and an untrusted network 84 is defined by the security officer at the NSC by defining multiple permitted profiles for a principal. When the principal authenticates at the security device 18 associated with this host 88, the principal determines which of the permitted profiles is to be used." Thus, Williams discloses that a user (security officer at the NSC) defines multiple permitted profiles for a principal and that based on the profiles the host operates on the second VPN or on an untrusted line. Williams does not perform a map change to associate a second memory map with a process thread whereby the second memory map provides different memory access with respect to a first memory map that is associated with the process thread. Nor does Williams restore the privilege level to a level that does not allow a map change.

In the present Office action, the Office action states, "[i]n response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986)." Office action, pgs. 21-22, secs. 92-93. Applicant strongly disagrees with the Office action's characterization of Applicant's response to the Office action dated December 21, 2004. In the amendment to the Office action dated December 21, 2004, the Applicant made several different arguments toward

In re Application of WILLMAN
Serial No. 09/915,628

this very point. For example, Applicant stated at pg. 25, line 15, "[t]hus, in any permissible combination, the cited references still fail to disclose or suggest applicant's invention." In another example, Applicant stated at pg. 30, line 4, "[a]s discussed above, the cited references, whether considered alone or in any permissible combination, do not disclose or suggest performing the map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread." As Applicant cited above, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Applicant merely accepted the Office action's admissions of the shortcomings of Magee and Williams, argued against the Office action's assertions of what Magee and Williams teach individually and in combination, and argued that neither piece of prior art by itself nor in any permissible combination can satisfy the requirements of a 35 U.S.C. § 103(a) rejection.

Additionally, in the present Office action, the Office action states, "[i]n response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., defining map change to be providing different memory access with respect to the first memory map) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)." Applicant respectfully disagrees with this assertion made in the Office action and respectfully requests the Examiner review the claims as filed in the response to the Office action dated December 21, 2004, as well as the claims as originally filed. Both as originally filed and as amended, claim 1 recited the phrase, "the second memory map providing different memory access

In re Application of WILLMAN
Serial No. 09/915,628

with respect to the first memory map.” Thus, Applicant was not arguing limitations that were not part of the claims and applicant respectfully requests that these grounds for rejection be dismissed.

Furthermore, the Office action again states, “Williams teaches mapping and switching back and forth between separate trusted and non-trusted systems (col. 26, lines 18-26) and thus satisfies the broadest reasonable interpretation of the claim language.” Office action, pg. 22, sec. 94. As argued above regarding this very cite, Williams teaches that a user (security officer at the NSC) defines multiple permitted profiles for a principal and that based on the profiles the host operates on the second VPN or on an untrusted line. Again, Williams does not perform a map change to associate a second memory map with a process thread whereby the second memory map provides different memory access with respect to a first memory map that is associated with the process thread. Nor does Williams restore the privilege level to a level that does not allow a map change. The office action further argues, “Williams teaches a map change to associate a second memory map by switching back and forth between a trusted and non-trusted system. It is inherent that there is a process or a thread to perform this particular feature. Both Williams and Magee teaches [sic] using thread processing. In Williams, two examples satisfy the broadest reasonable interpretation of privilege levels: trusted and non-trusted. Only trusted access will allow map change (col. 16, lines 60-67). Non-trusted will not allow it.” Office action pg. 23, sec. 95. Again, neither Williams nor Magee teach, disclose, or remotely hint at performing a map change to associate a second memory map with a process thread whereby the second memory map provides different memory access with respect to a first memory map that is associated with the process thread. Nor does any permissible combination of

In re Application of WILLMAN
Serial No. 09/915,628

Williams or Magee teach, disclose, or remotely hint at performing a map change to associate a second memory map with a process thread whereby the second memory map provides different memory access with respect to a first memory map that is associated with the process thread. At least for these additional reasons, claim 1 and the claims that depend thereon are patentable over the cited references.

In summary, the ability to switch between a trusted network and an untrusted network as defined by the security officer at the NSC by defining multiple permitted profiles for a principal is *not* receiving a request via a process thread having a first memory map associated therewith, changing a privilege level to a level that allows a map change, performing the map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread, and restoring the privilege level to a level that does not allow a map change. At least for these reasons, by law, claim 1 and the claims that depend thereon are patentable over the cited art, whether considered alone or in any permissible combination.

Moreover, the Office action does not provide proper motivation for combining Magee with the subject matter discussed in Williams. However, by law, in order to support a § 103(a) rejection, there must be some teaching, suggestion, or motivation other than applicant's teachings for modifying a cited reference or combining references to achieve the claimed invention. The Office action does not indicate any suggestion or motivation in the prior art of record, either explicit or otherwise, for modifying the references or combining the references in a manner that would achieve the claimed invention, or point out any teaching as to how such a modification or combination might be accomplished, or what might be accomplished thereby. Instead the Office action merely recites, "It would have

In re Application of WILLMAN
Serial No. 09/915,628

been obvious...to combine the feature of teach [sic] changing maps, performing the map change to associate a second memory map with the process thread, the second memory map providing different memory access with respect to the first memory map, and restoring the privilege level to a level that does not allow a map change to the existing system of Magee in order to increase the security and integrity of the system (col. 26, lines 18-26)." Office action, pgs. 4-5, sec. 4. Such broad, conclusory statements do not come close to adequately addressing the issue of motivation to combine, are not evidence of obviousness, and therefore are improper as a matter of law. *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Furthermore, the Office action states, "Williams and Magee are both in the same field of endeavor of computer processing and memory mapping, therefore, one of ordinary skill in the art of computer processing and memory mapping would have been able to combine the teachings of the two references." Office action, pg. 23, sec. 96. Again, the Office action does not indicate any suggestion or motivation in the prior art of record, either explicit or otherwise, for modifying the references or combining the references in a manner that would achieve the claimed invention, or point out any teaching as to how such a modification or combination might be accomplished, or what might be accomplished thereby. Such broad, conclusory statements as those presented in the Office action at pg. 23, sec. 96 do not come close to adequately addressing the issue of motivation to combine, are not evidence of obviousness, and therefore are improper as a matter of law. *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Again, the Office action does not indicate any suggestion or motivation in the prior art of record, either explicit or otherwise, for combining the references in a manner that

In re Application of WILLMAN
Serial No. 09/915,628

would achieve the claimed invention, and has failed to meet the requirement of establishing a case of *prima facie* obviousness. Further, any motivation for receiving a request via a process thread having a first memory map associated therewith, changing a privilege level to a level that allows a map change, performing the map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread, and restoring the privilege level to a level that does not allow a map change comes directly from applicant's teachings, not from any of the cited references. See applicant's disclosure, pg. 19, line 18 – pg. 20, line 10 and pg. 26, line 17 – pg. 28, line 4. It is well settled that such a hindsight reconstruction based on applicant's teachings is impermissible by law. In order to support a § 103(a) rejection, there must be some teaching, suggestion, or motivation other than applicant's teachings for modifying a cited reference or combining references to achieve the claimed invention.

Furthermore, the Office action states, "[t]he support for motivation is found in Williams on [sic] col. 26, lines 18-26. In response to applicant's argument that the examiner's conclusion of obviousness is based on improper hindsight reasoning, it must be recognized that any judgment on the obviousness is in a sense necessarily a reconstruction based on hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971)." Office action, pg. 24, sec. 97.

As argued above with respect to this very cite from Williams, the ability to switch between a trusted network and an untrusted network as defined by the security officer at the

In re Application of WILLMAN
Serial No. 09/915,628

NSC by defining multiple permitted profiles for a principal is *not* receiving a request via a process thread having a first memory map associated therewith, changing a privilege level to a level that allows a map change, performing the map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread, and restoring the privilege level to a level that does not allow a map change. Applicant submits that not only does the cited text not even remotely correspond to any of the elements of the claims, but further that it does not provide proper motivation for combining Williams with Magec thereby resulting in the attainment of the subject matter for claim 1. At least for these reasons, claim 1 and the claims that depend thereon are patentable over the cited art, whether considered alone or in any permissible combination by law.

Furthermore, even if the references could be permissibly combined by law in the manner suggested by the Office action (which applicants submit is not permissible), they would still fail to teach a method for performing a memory map change to associate a second memory map, that provides different memory access with respect to a first memory map, with the process thread as recited in claim 1. At least for this additional reason, claim 1 and the claims that depend thereon are patentable over the cited references.

Similarly and as previously argued, independent claims 32, 64, and 70 are patentable over the cited art. Claim 32 generally recites a process having at least one thread; a first memory map associated with the thread and having data therein that maps virtual memory addresses to physical memory; a second memory map having data therein that maps virtual memory addresses to physical memory, the second memory map providing different memory access with respect to the first memory map; a protection

In re Application of WILLMAN
Serial No. 09/915,628

mechanism, the protection mechanism configured to allow changing of a map; and trusted code, the trusted code configured to invoke the protection mechanism to change the thread from being associated with the first map to being associated with the second map.

Claim 64 generally recites associating first and second address maps with a process, wherein at least the second address map includes a mapping that maps a virtual address to a physical address that is larger than the largest possible virtual memory address; receiving a request from a thread of the process to change from the first address map to the second address map; changing the first address map to the second address map; and using the mapping to access data at a physical memory location having a physical address that is larger than the largest possible virtual memory address. Claim 70 generally recites associating first and second address maps with a process, wherein the second address map provides different memory access with respect to the first memory map; running trusted code with the first map; switching to the second map prior to running a first set of untrusted code without switching the process; and returning to the first map after completion of the untrusted code. As discussed above, the cited references, whether considered alone or in any permissible combination, do not disclose or suggest performing the map change to associate a second memory map that provides different memory access with respect to the first memory map with the process thread (e.g. the protection mechanism, the mapping, or the switching). Thus, claims 32, 64, and 70 and the claims that depend thereon are patentable over the cited references.

Turning to the rejection of dependent claims 6 and 35 of the present invention, the Office action rejected claims 6 and 35 under 35 U.S.C. § 103(a) as being unpatentable over Magee in view of Williams, and in further view of Gulsen. Again, Applicant respectfully

In re Application of WILLMAN
Serial No. 09/915,628

submits that the rejection of claim 6 and 35 are improper. Regarding claim 6, claim 6 depends from independent claim 1. For the reasons stated above with reference to claim 1, in any permissible combination, Magee and Williams do not disclose, teach, or even suggest the limitations of claim 1. Gulsen does not cure the deficiencies of Magee and Williams. Thus, any permissible combination of Magee, Williams, and Gulsen does not disclose or suggest the limitations of claim 6. At least for this reason, claim 6 is patentable over the cited references.

Regarding claim 35, claim 35 depends from independent claim 32. For the reasons stated above with reference to claim 32, in any permissible combination, Magee and Williams do not disclose, teach, or even suggest the limitations of claim 32. Gulsen does not cure the deficiencies of Magee and Williams. Thus, any permissible combination with Magee, Williams, and Gulsen does not disclose or suggest the limitation of claim 35. At least for this reason, claim 35 is patentable over the cited references.

For at least these reasons, applicant submits that all the claims are patentable over the prior art of record. Reconsideration and withdrawal of the rejections in the Office action is respectfully requested and early allowance of this application is earnestly solicited.

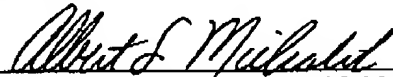
In re Application of WILLMAN
Serial No. 09/915,628

CONCLUSION

In view of the foregoing remarks, it is respectfully submitted that claims 1-30, 32-68, and 70-76 are patentable over the prior art of record. Applicant also respectfully submit that the application is in good and proper form for allowance. A favorable action on the part of the Examiner is earnestly solicited.

If in the opinion of the Examiner a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney at (425) 836-3030.

Respectfully submitted,



Albert S. Michalik, Reg. No. 37,395
Attorney for Applicant
Law Offices of Albert S. Michalik, PLLC
704 - 228th Avenue NE, Suite 193
Sammamish, WA 98074
(425) 836-3030
(425) 836-8957 (facsimile)

In re Application of WILLMAN
Serial No. 09/915,628

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this Amendment, along with transmittal, credit card payment form, petition for extension of time, and facsimile cover sheet, are being transmitted by facsimile to the United States Patent and Trademark Office in accordance with 37 C.F.R. 1.6(d) on the date shown below:

Date: October 26, 2005


Albert S. Michalik

2721 Second Amendment